

ABSTRACT OF THE DISCLOSURE

A thorough method for restricting which operations (processes) can be run by a user on a single workstation computer or by a user on a session in a multi-user environment, such as Microsoft Windows 2000 Terminal Services. By default, all applications (processes) are disallowed. Only explicitly assigned applications (processes) are allowed to run. The method entails running two software modules in user mode, one of which maintains a list of allowed processes for each user and one of which monitors new processes as they are started. When a new process is started the monitoring module sends the process ID to the list module. The list module checks the ID against its list and kills the process if it is not authorized. This way, only processes created by users are validated as apposed to validating all file I/O (processor intensive). This decreases the processing requirements.

RWC/rwk